AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Previously presented) A method of establishing a path for distributing data through a network, comprising:

establishing a first data distribution path through the network, the network comprising at least one switch and one link;

determining whether eavesdropping has occurred on the first data distribution path using quantum cryptography; and

establishing a second data distribution path through the network based on the eavesdropping determination, wherein the second data distribution path comprises a different route through the network than the first data distribution path.

2. (Original) The method of claim 1, wherein the network comprises an optical network.

3. (Original) The method of claim 1, wherein the at least one switch comprises at least one optical switch.

4. (Original) The method of claim 1, wherein the at least one link comprises at least one optical link.

5. (Original) The method of claim 1, wherein the first data distribution path comprises a plurality of links and switches.

6. (Original) The method of claim 5, wherein the second data distribution path comprises a plurality of links and switches.

7. (Original) The method of claim 6, wherein the first data distribution path and the second data distribution path comprise no common links and switches.

8. (Original) The method of claim 6, wherein the first data distribution path and the second data distribution path comprise a subset of common links and switches.

9. (Original) The method of claim 1, wherein the first data distribution path comprises a first encryption key distribution path.

10. (Original) The method of claim 1, wherein the second data distribution path comprises a second encryption key distribution path.

11. (Original) The method of claim 9, further comprising:

distributing a first encryption key via the first encryption key distribution path.

12. (Original) The method of claim 10, further comprising:

distributing a second encryption key via the second encryption key distribution path.

13. (Previously presented) A computer-readable medium containing instructions for controlling at least one processor to perform a method of establishing a path for distributing data through a network, the method comprising:

initiating establishment of a first data distribution path through the network, the network comprising at least one switch and one link;

determining whether eavesdropping has occurred on the first data distribution path using quantum cryptography; and

initiating establishment of a second data distribution path through the network based on the eavesdropping determination, wherein the second data distribution path comprises a different route through the network than the first data distribution path.

14. (Previously presented) A system for establishing a path for distributing data through a network, comprising:

means for establishing a first data distribution path through the network, the network comprising at least one switch and one link;

means for determining whether eavesdropping has occurred on the first data distribution path using quantum cryptography; and

means for establishing a second data distribution path through the network based on the eavesdropping determination, wherein the second data distribution path comprises a different route through the network than the first data distribution path.

15. (Original) A system for establishing a path for distributing data through a network, comprising:

a switch configured to establish a first encryption key distribution path through the network, the first encryption key distribution path comprising a plurality of switches and links; and

a data distribution endpoint configured to determine whether eavesdropping has occurred on the first encryption key distribution path using quantum cryptography,

wherein the switch is further configured to establish a second encryption key distribution path through the network responsive to the eavesdropping determination, the second encryption key distribution path comprising a plurality of switches and links.

16-32. (Canceled)

33. (Previously presented) A method of routing around eavesdroppers in a network, comprising:

establishing a first path in the network;

transmitting data symbols over the first path;

identifying eavesdropping on the first path using quantum cryptography;

establishing a second path in the network responsive to the eavesdropping identification, wherein the second path comprises a different route through the network than the first path; and

transmitting data symbols over the second path.

34. (Original) The method of claim 33, wherein the network comprises an optical network.

35. (Original) The method of claim 33, wherein the at least one switch comprises at least one optical switch.

36. (Original) The method of claim 33, wherein the at least one link comprises at least one optical link.

37. (Original) The method of claim 33, wherein the first path comprises a plurality of links and switches.

38. (Original) The method of claim 37, wherein the second path comprises a plurality of links and switches.

39. (Original) The method of claim 38, wherein the first path and the second path comprise no common links and switches.

40. (Original) The method of claim 38, wherein the first path and the second path comprise a subset of common links and switches.

41. (Original) The method of claim 33, wherein the data symbols comprise at least a portion of an encryption key.

42. (Original) The method of claim 33, wherein the data symbols comprise polarized photons.

43. (Original) A quantum encryption key distribution device, comprising:
a transceiver; and
a processing unit configured to:
establish a first key distribution path in the network, the first key distribution path comprising a plurality of links and switches,
transmit at least a portion of a first encryption key over the first key distribution path via the transceiver,

identify eavesdropping on the first key distribution path using quantum cryptographic techniques,

establish a second key distribution path in the network responsive to the eavesdropping identification, the second key distribution path comprising a plurality of links and switches, and

transmit at least a portion of a second encryption key over the second key distribution path via the transceiver.

44. (Previously presented) A system for routing around eavesdroppers in a network, comprising:

means for establishing a first path in the network;

means for transmitting data symbols over the first path;

means for identifying eavesdropping on the first path using quantum cryptography;

means for establishing a second path in the network responsive to the eavesdropping identification, wherein the second path comprises a different route through the network than the first path; and

means for transmitting data symbols over the second path.

45-53. (Canceled)